2階算術におけるヒルベルトの零点定理 (圏論と証明論の新たな融合を目指して)

AUTHOR(S):

坂本, 伸幸

CITATION:

坂本, 伸幸. 2階算術におけるヒルベルトの零点定理 (圏論と証明論の新たな融合を目指して). 数理解析研究所講究録 2001, 1217: 86-97

ISSUE DATE:

2001-06

URL:

http://hdl.handle.net/2433/41234

数理解析研究所講究録 1217 巻 2001 年 86-97

2階算術におけるヒルベルトの零点定理

東北大学大学院理学研究科数学専攻
坂本 伸幸 (SAKAMOTO, Nobuyuki)

概 要

ここでは，ヒルベルトの零点定理の原始的，構成的な証明を紹介し，それと2階算術における複素数に関する充足論理式 [3] を用いて，2階算術の部分体系でヒルベルトの零点定理を証明する．

代数閉体のすべての定理は2階算術の部分体系 RCA_0 における複素数に関して成り立つという定理が，シンプソン，田中，山崎によって証明されている ([3] 参照)．この定理を用いて，2階算術でヒルベルトの零点定理を証明する．このとき，代数閉体の体系のヒルベルトの零点定理を表す論理式は多項式の個数や次数，変数の個数に依存してしまうので，RCA_0 で，それらすべての論理式が代数閉体の公理のみから証明できることを見る必要があるが，それには証明が原始再帰的に得られることを見れば十分である．また，2階算術で，ヒルベルトの零点定理を証明するのにどの程度強い公理が必要かという問題は，複素数（実数）の充足論理式に関する未解決問題と関係し，未だ解決されていないが，充足論理式が強い充足条件を満たすことが証明できる体系であればヒルベルトの零点定理が証明できること，RCA_0 においても、変数の数に関し“数値別”には証明できることはわかる．

1 代数閉体

まず,(標数0の）代数閉体の体系を定義する．この定義は通常のそれとは割り算が全域的であるという点で少し異なるものである．

定義 1.1 (ACF(0))**.** 言語 $\mathcal{L}_{\mathsf{AF}}$ は体の言語（$\langle +, -, \cdot, /, 0, 1, = \rangle$）とする．体系 AF は

言語が $\mathcal{L}_{\mathsf{AF}}$ で，以下の公理を持つものとする．

$$x+0=x,\quad x+y=y+x,\quad x+(y+z)=(x+y)+z,\quad x+(-x)=0$$
$$x\cdot 0=0,\quad x\cdot 1=x,\quad x\cdot y=y\cdot x,\quad x\cdot(y\cdot z)=(x\cdot y)\cdot z$$
$$x/0=0,\quad x\neq 0\to x\cdot(y/x)=y$$
$$1\neq 0,\quad x\cdot(y+z)=(x\cdot y)+(x\cdot z)$$

ACF(0) は AF に以下の公理を加えたものとする．

$$\overbrace{1+1+\cdots+1}^{n\text{個}}\neq 0\quad(n\geq 2)$$
$$\forall x_0\forall x_1\cdots\forall x_n\exists y(x_n\neq 0\to x_0+x_1y+\cdots+x_ny^n=0)\quad(n\geq 1)$$

ACF(0) においては，

$$x/x=\begin{cases}0 & x=0\text{のとき}\\ 1 & x\neq 0\text{のとき}\end{cases}$$

が成り立つ．すなわち，項が 0 か否かで場合分けができる．以降，加減乗除と 0 か否かでの場合分けだけで実現できる計算のことを**Z計算**と呼ぶことにする．

ACF(0) において，多項式 $\Sigma a_{k_0,k_1,\ldots,k_m}x_0^{k_0}x_1^{k_1}\cdots x_m^{k_m}$ は，単に数の（有限）列 $\langle a_{k_0,k_1,\ldots,k_m}\rangle_{k_0,k_1,\ldots,k_m}$ で表す．多項式同士の積，一変数多項式同士の商，剰余は Z 計算で求められる．さらに，ユークリッドの互除法も Z 計算によって実現され，特に，複数の一変数多項式の最大公約元も Z 計算で求められる．さらに次のこともいえる．

定理 1.2 (ヒルベルトの零点定理). $n\in\mathbb{N}$ とする．各 $l<n$ について，多項式 p_l を表す変数の列 $\langle a^l_{k_0,k_1,\ldots,k_m}\rangle_{k_0,k_1,\ldots,k_m}$ が与えられたとき，これらの変数をもつ ACF(0) の項の列の列 $\langle\langle t^l_{k_0,k_1,\ldots,k_m}\rangle_{k_0,k_1,\ldots,k_m}:l<n\rangle$ が原始再帰的にとれ，それらが表す多項式 $q_0,q_1,\ldots,q_{n-1}$ について

$$\mathsf{ACF}(0)\vdash p_0(\vec{x})q_0(\vec{x})+\cdots+p_{n-1}(\vec{x})q_{n-1}(\vec{x})=1$$

がいえる．また，上の $\mathsf{ACF}(0)\vdash\cdots$ の証明も原始再帰的に得られる．

この定理の証明は 3 節で行う．

任意の代数閉体 F に対し，F 係数多変数多項式に関するヒルベルトの零点定理が成立し，定理の主張の中の多項式 q_i の次数の上界が p_i たちの次数から求められることはよく知られている．これから，完全性定理により "ACF(0) $\vdash$ 高々 n 次の多項式に関するヒルベルトの零点定理" の証明が存在することはわかる．しかし，q_i たちが Z 計算で求められること，証明が原始再帰的に得られることを見るには 3 節のような直接的な議論が必要になる．

2 RCA_0 における複素数

2 階算術の部分体系で，自然数上の演算に関する基本的な公理と Σ^0_1 帰納法，Δ^0_1 内包公理からなるものを RCA_0 と呼んだ．2 階算術と，その部分体系である RCA_0 などについては [2] を参照のこと．

以下，RCA_0 で ACF(0) が形式化されているとし（項，論理式，証明が自然数にコード化されている），その際の ACF(0) の変数は $v_0, v_1, \ldots$ であるとする．また，t' を t の部分項とするとき，t' のコードは t のコードより小さいとしておく．さらに，ACF(0) の体系の論理式とその RCA_0 におけるコードを自然に同一視する．そして，任意の無限複素数列 E，複素数 A に対し，E^i_A で E の i 番目の複素数を A に置き換えて得られる複素数列を表すとする．無限実数列 E と実数 A に対しても同様の定義をする．

定義 2.1 (l 解釈列). 無限複素数列 $E = \langle E_0, E_1, \ldots \rangle$，自然数 l に対し，有限複素数列

$$V_E = \langle V_E(s) : s < l, s \text{ は ACF(0) の項のコード} \rangle$$

が環境 E における l 解釈列であるとは，

$$V_E(0) = 0, \quad V_E(1) = 1$$
$$V_E(v_i) = (E)_i$$
$$V_E(t_1 + t_2) = V_E(t_1) + V_E(t_2), \quad V_E(-t) = -V_E(t)$$
$$V_E(t_1 t_2) = V_E(t_1) V_E(t_2), \quad V_E(t_1/t_2) = V_E(t_1)/V_E(t_2)$$

が成り立つことをいう．

以下の定理は，複素数に関する基本的な演算が RCA_0 でできることを主張する．この定理に関しては，[3] を参照のこと．

定理 2.2. RCA_0で以下の主張がいえる．任意の無限複素数列E，自然数lに対し，l解釈列が存在する．しかも，l解釈列は次の意味で一意である：V_Eが環境Eにおけるl解釈列で，$V'_{E'}$が環境E'におけるl'解釈列であり，項sのコードがlとl'より小さく，sに現れる自由変数を$v_{i_0}, v_{i_1}, \ldots, v_{i_j}$とするとき，

$$(E)_{i_0} = (E')_{i_0}, (E)_{i_1} = (E')_{i_1}, \ldots .(E)_{i_j} = (E')_{i_j}$$

が成り立つならば，

$$V_E(s) = V'_{E'}(s)$$

□

さらに，次の充足論理式に関する結果がある．この定理についても [3] を参照のこと．

定理 2.3 (充足論理式). 以下を満たすRCA_0のΔ^0_2論理式$\mathrm{SAT}_{\mathbb{C}}(x, E)$が存在する：$\mathrm{SAT}_{\mathbb{C}}$は“タルスキの充足条件”を満たす．すなわち，

$$\begin{aligned}
\mathrm{SAT}_{\mathbb{C}}(t_1 = t_2, E) &\Leftrightarrow \text{ある } l \text{ 解釈列 } V_E \text{に対し}, V_E(t_1) = V_E(t_2) \\
&\Leftrightarrow \text{任意の } l \text{ 解釈列 } V_E \text{に対し}, V_E(t_1) = V_E(t_2) \\
\forall i \leq n \mathrm{SAT}_{\mathbb{C}}(\varphi_i, E) &\Leftrightarrow \mathrm{SAT}_{\mathbb{C}}(\varphi_0 \wedge \varphi_1 \wedge \cdots \wedge \varphi_n, E) \\
\exists i \leq n \mathrm{SAT}_{\mathbb{C}}(\varphi_i, E) &\Leftrightarrow \mathrm{SAT}_{\mathbb{C}}(\varphi_0 \vee \varphi_1 \vee \cdots \vee \varphi_n, E) \\
\neg \mathrm{SAT}_{\mathbb{C}}(\varphi, E) &\Leftrightarrow \mathrm{SAT}_{\mathbb{C}}(\neg\varphi, E) \\
\forall A \in \mathbb{C}(\mathrm{SAT}_{\mathbb{C}}(\varphi, E^i_A)) &\Leftrightarrow \mathrm{SAT}_{\mathbb{C}}(\forall v_i \varphi, E) \\
\exists A \in \mathbb{C}(\mathrm{SAT}_{\mathbb{C}}(\varphi, E^i_A)) &\Leftrightarrow \mathrm{SAT}_{\mathbb{C}}(\exists v_i \varphi, E)
\end{aligned}$$

さらに，

$$(\mathsf{ACF}(0) \vdash \varphi) \Leftrightarrow \forall E \in \mathbb{C}^{\mathbb{N}} \mathrm{SAT}_{\mathbb{C}}(\varphi, E)$$

が成立する．そして，任意の$E, E' \in \mathbb{C}^{\mathbb{N}}$と$\varphi$について，各$i$に対し「$v_i$が$\varphi$に自由に現れるならば$(E)_i = (E')_i$」となるならば

$$\mathrm{SAT}_{\mathbb{C}}(\varphi, E) \Leftrightarrow \mathrm{SAT}_{\mathbb{C}}(\varphi, E')$$

さて，この定理と定理1.2をあわせると，次の系が得られる．

系 2.4 (2階算術におけるヒルベルトの零点定理・"数値別"ヴァージョン). 任意の自然数mに対し，RCA_0で以下の主張が示せる．$\vec{x}=(x_0,x_1,\ldots,x_{m-1})$とする．$p_0(\vec{x}),\ldots,p_{n-1}(\vec{x})$を複素数係数多変数多項式で，共通根を持たないものとする．このとき，ある$q_0(\vec{x}),\ldots,q_{n-1}(\vec{x})\in\mathbb{C}[\vec{x}]$を用いて

$$p_0(\vec{x})q_0(\vec{x})+\cdots+p_{n-1}(\vec{x})q_{n-1}(\vec{x})=1$$

とできる．

証明 定理1.2で主張しているRCA_0で証明できる$\mathsf{ACF}(0)$の命題は

$$\forall x_0\forall x_1\cdots\forall x_{m-1}((x_0,x_1,\ldots,x_{m-1})\text{は}p_j\text{たちの共通根でない})\to\psi$$

の形で，ψは$p_0(x)q_0(x)+\cdots+p_{n-1}(x)q_{n-1}(x)=1$なることをあらわす量化記号を含まない論理式である．ここに，q_iたちはp_iたちの係数を自由変数にもつ項で表されている．よって，$p_0(\vec{x}),\ldots,p_{n-1}(\vec{x})$が共通根を持たないならば，$p_i$たちの係数を適当に並び替えたものを$E$とし，定理2.3を$m$回適用することによって$\mathrm{SAT}_{\mathbf{C}}(\forall x_0\forall x_1\cdots\forall x_{m-1}(x_i\text{たちは}p_j\text{たちの共通根でない}),E)$を得る．よって，$\mathrm{SAT}_{\mathbf{C}}(\psi,E)$．題意が示せた． □

次の論理式をSSCで表す．

$$\forall n[\mathrm{SAT}_{\mathbf{R}}(\exists v_{i_0}\exists v_{i_1}\cdots\exists v_{i_{n-1}}\varphi,E)\Rightarrow\exists A\in\mathbb{R}^n(\mathrm{SAT}_{\mathbf{R}}(\varphi,E^{i_0,i_1,\ldots,i_{n-1}}_{(A)_0,(A)_1,\ldots,(A)_{n-1}}))]$$

ただし，$E^{i_0,i_1,\ldots,i_{n-1}}_{(A)_0,(A)_1,\ldots,(A)_{n-1}}$は，各$k$に対し，$E$の$i_k$番目を$(A)_{i_k}$で置き換えたものを表す．SSCに関しては，

$$\mathsf{RCA}_0+\Sigma^0_2\text{-}\mathsf{BDC}\vdash\mathsf{SSC}$$

がわかる[3]．ここに，Σ^0_2-BDCは

$$\forall n\forall X\exists Y\varphi(n,X,Y)\to\forall l\exists Z\forall n<l\varphi(n,(Z)_n,(Z)_{n+1})$$

(φはΣ^0_2で，Zを自由変数として含まない)なる公理図式である．RCA_0のみからSSCが導かれることが予想されているが，未だ解決されていない．SSCがあれば，系2.4より強い結果が得られる．

定理 2.5 (2階算術におけるヒルベルトの零点定理). SSCを導出できる2階算術の部分体系（例えば $\mathsf{RCA}_0 + \Sigma^0_2\text{-BDC}$）で以下の主張が示せる．$m \in \mathbf{N}$ とし，$\vec{x} = (x_0, x_1, \ldots, x_{m-1})$ とする．$p_0(\vec{x}), \ldots, p_{n-1}(\vec{x})$ を複素数係数多変数多項式で，共通根を持たないものとする．このとき，ある $q_0(\vec{x}), \ldots, q_{n-1}(\vec{x}) \in \mathbb{C}[\vec{x}]$ を用いて

$$p_0(\vec{x})q_0(\vec{x}) + \cdots + p_{n-1}(\vec{x})q_{n-1}(\vec{x}) = 1$$

とできる． □

3 定理1.2の証明

本定理の証明は，[1]，[4] にあるような構成的な証明を形式化する事によって実現される．ここでは，形式化する以前の素朴な証明を紹介し，ところどころ形式化の要点を述べるにとどめる．まず，この証明に必要な定義，命題を準備する．

定義 3.1 (2つの多項式に対する終結式). 一変数複素数係数多項式 $p(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_0, q(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0$ $(a_m, b_n \neq 0)$ に対し，これらのシルベスター行列 $\mathrm{Syl}(p, q, x)$ を

$$\begin{pmatrix}
a_m & 0 & \cdots & 0 & b_n & 0 & \cdots & 0 \\
a_{m-1} & a_m & \cdots & 0 & b_{n-1} & b_n & \cdots & 0 \\
\vdots & \vdots & \ddots & a_m & \vdots & \vdots & \ddots & b_n \\
 & \vdots & \ddots & a_{m-1} & & \vdots & \ddots & b_{n-1} \\
a_0 & a_1 & & & b_0 & b_1 & & \\
0 & a_0 & & \vdots & 0 & a_0 & & \vdots \\
\vdots & 0 & & & \vdots & 0 & & \\
 & & \ddots & & & & \ddots & \\
0 & 0 & & a_0 & 0 & 0 & & b_0
\end{pmatrix}$$

で定め，p, q の x に関する**終結式** $\mathrm{Res}(p, q, x)$ を

$$\det \mathrm{Syl}(p, q, x)$$

で定める．p, q が $x, x_0, x_1, \ldots, x_n$ を変数にもつ多変数多項式であってもこれらを $\mathbb{C}[x_0, x_1, \ldots, x_n]$ を係数にもつ x に関する一変数多項式と見て同様に $\mathrm{Syl}(p, q, x), \mathrm{Res}(p, q, x)$ が定義できる．

注意 3.2. p, q を $x, x_0, x_1, \ldots, x_n$ を変数にもつ多変数多項式で，

$$p = r(x_0, x_1, \ldots, x_n)x^N + (x \text{ に関する次数が } N \text{ 未満の項})$$

であったとする．$x_0, x_1, \ldots, x_n$ に複素数 $c_0, c_1, \ldots, c_n$ を代入すると r が 0 になるとすれば，一般に

$$[\mathrm{Res}(p(x, x_0, x_1, \ldots, x_n), q(x, x_0, x_1, \ldots, x_n), x) \text{ の各 } x_i \text{ に } c_i \text{ を代入したもの}]$$
$$= \mathrm{Res}(p(x, c_0, c_1, \ldots, c_n), q(x, c_0, c_1, \ldots, c_n), x)$$

は成り立たない．すなわち，終結式をとる前に変数に複素数を代入するのと終結式をとった後で変数に複素数を代入するのでは結果が異なることがある．

シルベスター行列に関して，次の命題が成り立つことが直ちにわかる．

命題 3.3. $p(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_0, q(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0$ $(a_m, b_n \neq 0)$ に対し，

$$(x^{m+n-1}, x^{m+n-2}, \ldots, 1)\mathrm{Syl}(p, q, x) = (x^{n-1}p, x^{n-2}p, \ldots, p, x^{m-1}q, x^{m-2}q, \ldots, q)$$

□

終結式は次の性質を持つ．

命題 3.4. 一変数多項式 p, q に対し，$\mathrm{Res}(p, q, x) = 0$ ならば p と q は共通根をもつ．

証明 $\mathrm{Res}(p, q, x) = 0$ ならば，$d_0, d_1, \ldots, d_{m+n-1} \in \mathbb{C}$ で，d_i のうち少なくとも 1 つは

$$d_0\begin{pmatrix} a_m \\ a_{m-1} \\ \vdots \\ a_0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + d_1\begin{pmatrix} 0 \\ a_m \\ \vdots \\ a_1 \\ a_0 \\ \\ 0 \end{pmatrix} + \cdots + d_{n-1}\begin{pmatrix} 0 \\ \vdots \\ 0 \\ a_m \\ a_{m-1} \\ \vdots \\ a_0 \end{pmatrix}$$

$$+ d_n\begin{pmatrix} b_n \\ b_{n-1} \\ \vdots \\ b_0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + d_{n+1}\begin{pmatrix} 0 \\ b_n \\ \vdots \\ b_1 \\ b_0 \\ \\ 0 \end{pmatrix} + \cdots + d_{m+n-1}\begin{pmatrix} 0 \\ \vdots \\ 0 \\ b_n \\ b_{n-1} \\ \vdots \\ b_0 \end{pmatrix} = 0$$

を成り立たせるものがとれる．これと命題3.3から，

$$\Big[\sum_{k=0}^{n-1} d_k x^{n-k-1}\Big]p(x) + \Big[\sum_{k=n}^{n+m} d_k x^{m+n-k}\Big]q(x) = 0$$

を得る．$p^\star = \sum_{k=0}^{n-1} d_k x^{n-k-1}, q^\star = \sum_{k=n}^{n+m} d_k x^{m+n-k}$ とおけば，$p^\star p = -q^\star q$．辺々一次式の積に分解して次数を比較することにより p, q が共通根を持つことがわかる．□

この証明の形式化の際，d_i は p, q の係数からZ計算で求められることに注意．

命題 3.5. $x, x_0, x_1, \ldots, x_n$ を変数にもつ多変数多項式 p, q に対し，ある多変数多項式 $p^\star, q^\star \in \mathbb{C}[x, x_0, x_1, \ldots, x_n]$ があって，

$$p^\star p + q^\star q = \mathrm{Res}(p, q, x)$$

が成り立つ．

証明 $\mathrm{Res}(p, q, x)$ が0のときは $p^\star = q^\star = 0$ とすればよい．

そうでないとき，命題3.3により

$$(x^{m+n-1}, x^{m+n-2}, \ldots, 1) = (x^{n-1}p, x^{n-2}p, \ldots, p, x^{m-1}q, x^{m-2}q, \ldots, q)(\mathrm{Syl}(p, q, x))^{-1}$$

ここで，クラーメルの公式より $(\mathrm{Syl}(p,q,x))^{-1} = \mathrm{Res}(p,q,x)^{-1}(\mathrm{Syl}(p,q,x))^{\sim}$ ．ここに，$((\mathrm{Syl}(p,q,x)))^{\sim}$の各成分は $\mathrm{Syl}(p,q,x)$ の成分（つまり p,q の係数）からなるある行列の行列式である．以上により，

$$\mathrm{Res}(p,q,x)(x^{m+n-1}, x^{m+n-2}, \ldots, 1) = (x^{n-1}p, x^{n-2}p, \ldots, p, x^{m-1}q, x^{m-2}q, \ldots, q)(\mathrm{Syl}(p,q,x))^{\sim}$$

第 $m+n$ 成分を比較して，ある $p^*, q^* \in \mathbb{C}[x, x_0, x_1, \ldots, x_n]$ に対し，$\mathrm{Res}(p,q,x) = p^*p + q^*q$ なることを得る． □

ここで，終結式という概念を複数の多項式にまで拡張しよう．

定義 3.6 (複数の多項式に対する終結式). x を変数にもつ一変数複素数係数多項式 $p_0, p_1, \ldots, p_n$に対し，多変数多項式 $q = u_1p_1 + \cdots + u_np_n \in \mathbb{C}[x, u_1, \ldots, u_n]$ を考え，p_0と q の終結式 $r = \mathrm{Res}(p_0, q, x) \in \mathbb{C}[u_1, \ldots, u_n]$ をとる．そして，r の $u_1^{i_1}u_2^{i_2}\cdots u_n^{i_n}$ の係数を

$$\mathrm{Res}_{i_1,i_2,\ldots,i_n}(p_0, p_1, \ldots, p_n, x)$$

とする．$\mathrm{Res}_{i_1,i_2,\ldots,i_n}(p_0, p_1, \ldots, p_n, x)$ たちを $p_0, p_1, \ldots, p_n$の**終結式**と呼ぶ．多変数複素数係数多項式$p_0, p_1, \ldots, p_n$に対しても同様に終結式が定義できる．

この終結式も 2 つの多項式に対する終結式と同様の性質を持つ．

命題 3.7. $p_0, p_1, \ldots, p_n \in \mathbb{C}[x]$ の終結式たちがすべて 0 ならば $p_0, p_1, \ldots, p_n$は共通根をもつ．

証明 このとき，$\mathrm{Res}(p_0, u_1p_1+\cdots+u_np_n, x)$ は（多項式として）0になる．$u_1p_1+\cdots+u_np_n$の x に関する次数を k とする．各 $a_1, a_2, \ldots, a_n \in \mathbb{C}$ に対し，$a_1p_1 + \cdots + a_np_n$ の x に関する次数が k ならば，$\mathrm{Res}(p_0, a_1p_1 + \cdots + a_np_n, x) = 0$ となるから（注意 3.2 も見よ），p_0と $a_1p_1 + \cdots + a_np_n$は共通根を持つ．p_0の根全体を $z_0, z_1, \ldots, z_d$とする．そして，

$$b_n = d+2, b_{n-i} = \begin{pmatrix} b_{n-i+1}b_{n-i+2}\cdots b_n \\ 2 \end{pmatrix} + 1$$

$(i = 1, 2, \ldots, n-2)$ と定める．各 $j_n \in \{1, 2, \ldots, b_n\}, j_{n-1} \in \{1, 2, \ldots, b_{n-1}\}, \ldots, j_2 \in \{1, 2, \ldots, b_2\}$ に対し，p_0と $p_1+j_2(p_2+j_3(\cdots(p_{n-1}+j_np_n)\cdots))$ との共通根を $z_{k_{j_2,j_3,\ldots,j_n}}$

とする．ここで，必要ならば j_nの動く範囲を変更することによって $p_1 + j_2(p_2 + j_3(\cdots(p_{n-1} + j_n p_n)\cdots))$ の x に関する次数は k であるとしてよい．このとき，鳩の巣原理により，$m \in \{2,3,\ldots,n\}$，長さ $n-m+1$ の 0-1 列 $i_m, i_{m+1}, \ldots, i_n$ に対し，$l^m_{i_m,i_{m+1},\ldots,i_n} \in \{1,2,\ldots,b_m\}$ を上手く選んで，$l^m_{0,i_{m+1},\ldots,i_n} \neq l^m_{1,i_{m+1},\ldots,i_n}$ であって，p_0 と

$$p_1 + l^2_{i_2,i_3,\ldots,i_n}(p_2 + l^3_{i_3,i_4,\ldots,i_n}(\cdots(p_{n-1} + l^n_{i_n}p_n)\cdots))$$

が $i_2, i_3, \ldots, i_n$に依らない共通根 $c = z_k$を持つようにできる．このとき，任意の長さ $n-2$ の 0-1 列 $i_3, i_4, \ldots, i_n$ に対し，$p_1 + l^2_{0,i_3,\ldots,i_n}(p_2 + l^3_{i_3,\ldots,i_n}(\cdots(p_{n-1} + l^n_{i_n}p_n)\cdots))$，$p_1 + l^2_{1,i_3,\ldots,i_n}(p_2 + l^3_{i_3,\ldots,i_n}(\cdots(p_{n-1} + l^n_{i_n}p_n)\cdots))$ が共に根 c を持つのだから，$(l^2_{0,i_3,\ldots,i_n} - l^2_{1,i_3,\ldots,i_n})(p_2 + l^3_{i_3,\ldots,i_n}(\cdots(p_{n-1} + l^n_{i_n}p_n)\cdots))$ も根 c を持つ．$l^2_{0,i_3,\ldots,i_n}$ と $l^2_{1,i_3,\ldots,i_n}$ は相違なるのだから $p_2 + l^3_{i_3,\ldots,i_n}(\cdots(p_{n-1} + l^n_{i_n}p_n)\cdots)$ が根 c を持つことがわかる．$i_3 = 0,1$ に対し同様の議論を適用して $p_3 + l^4_{i_4,\ldots,i_n}(\cdots(p_{n-1} + l^n_{i_n}p_n)\cdots)$ が根 c を持つことがわかる．以下同様にして p_nが根 c を持つことがわかる．これから，p_{n-1}も根 c を持ち，$\cdots$, p_2も根 c を持つことがわかる． □

この議論を形式化する際，多項式の根は Z 計算で求められないが，根を ACF(0) の項で書き下す必要はないので問題はない．次の性質は複数の多項式に対する終結式の定義と命題 3.5 から直ちにわかる．

命題 3.8. 多変数複素数係数多項式 $p_0, p_1, \ldots, p_n \in \mathbb{C}[x, x_0, \ldots x_m]$ に対し，各 $\mathrm{Res}_{i_1,i_2,\ldots,i_n}(p_0, p_1, \ldots, p_n, x)$ は

$$p_0^\star p_0 + p_1^\star p_1 + \cdots + p_n^\star p_n$$

$(p_0^\star, p_1^\star, \ldots, p_n^\star \in \mathbb{C}[x, x_0, \ldots x_m])$ の形で表せる． □

さて，定理の証明に戻ろう．与えられた多変数多項式 $p_0, p_1, \ldots, p_{n-1}$の変数 x_0に関する終結式 $r_0, r_1, \ldots, r_k$をとる．そして，r_iたちに現れる変数 x_jのうち，添え字 j が最小のものをとる．適当に変数変換

$$x_j = \tilde{x}_j, x_{j+1} = \tilde{x}_{j+1} + a_{j+1}\tilde{x}_j, x_{j+2} = \tilde{x}_{j+2} + a_{j+2}\tilde{x}_j, \ldots,$$

$(a_{j+1}, a_{j+2}, \ldots$は複素数$)$ を行って，r_0を x_jに関する多項式と見るとき

$$r_0 = cx_j^N + (x_j\text{に関する次数が } N \text{ 未満の項})\cdots (*)$$

(cは0でない複素数) となるようにできる．実際，まずは$a_{j+1}, a_{j+2}, \ldots$を変数記号と見てr_0に変数変換$x_j = \tilde{x}_j, x_{j+1} = \tilde{x}_{j+1} + a_{j+1}\tilde{x}_j, x_{j+2} = \tilde{x}_{j+2} + a_{j+2}\tilde{x}_j, \ldots$, をほどこせば，$r_0$はある多項式$d$に対して，$r_0 = d(a_{j+1}, a_{j+2}, \ldots)x_j^N +$ (x_jに関する次数がN未満の項) とかける．$d(a_{j+1}, a_{j+2}, \ldots)$を0にしないような複素数$a_{j+1}, a_{j+2}, \ldots$はZ計算で求められる．さらに，十分大きな自然数$M$をとり，$r_1, r_2, \ldots$に$x^M r_0$を加えることによって$r_1, r_2, \ldots$も（$*$）の形になるようにできる．さらに，$r_0, r_1, \ldots$の終結式をとり，この終結式たちに同様の変形を施す．この操作を行うたびに変数の数が減っていくから，いつかはでてくる終結式たちがすべて複素数になる．

$s_0, s_1, \ldots, s_{k'}$たちに対して変数x_jに関する終結式をとった際にその終結式たちがすべて0であったとする．このとき，$s_0, s_1, \ldots, s_{k'}$のx_j以外の変数にすべて0を代入したものの終結式たちもすべて0となる．この際に，s_iたちを（$*$）の形に変形しておいたので注意3.2のような問題は発生しない．これから，命題3.7により$s_0, s_1, \ldots, s_{k'}$は共通根$\vec{c}$を持つことがわかる．$s_0, s_1, \ldots, s_{k'}$が$s'_0, s'_1, \ldots$の$x_{j'}$に関する終結式であるとする．このとき$x_j, x_{j+1}, \ldots$に$\vec{c}$を代入し，$x_{j'+1}, x_{j'+2}, \ldots$に0を代入したものたちの$x_{j'}$に関する終結式たちも0である．よって，$s'_0, s'_1, \ldots$は共通根を持つ．このような議論を繰り返し適用することにより，結局$p_0, p_1, \ldots, p_{n-1}$が共通根を持つことがわかる．これは仮定に矛盾する．

よって，上のように終結式をとっていく操作を繰り返すうちにいつかは0でない複素数が終結式のなかに現れるときがある．$s_0, s_1, \ldots, s_{k'}$たちに対して変数x_jに関する終結式をとった際にその終結式の1つが0でない複素数であったとする．命題3.8により，ある多項式$s_0^\star, s_1^\star \ldots, s_{k'}^\star$を用いて

$$s_0^\star s_0 + s_1^\star s_1 + \cdots + s_{k'}^\star s_{k'} = 1$$

とかける．さらに，s_iたちは多項式$t_0, t_1, \ldots, t_{k''}$の終結式であったから，ある$t_0^\star, t_1^\star \ldots$, $t_{k''}^\star$を用いて

$$t_0^\star t_0 + t_1^\star t_1 + \cdots + t_{k''}^\star t_{k''} = 1$$

と書けることがわかる．この議論を繰り返し適用することによって，ある$p_0^\star, p_1^\star, \ldots$, $p_{n-1}^\star$を用いて

$$p_0^\star p_0 + p_1^\star p_1 + \ldots, p_{n-1}^\star p_{n-1} = 1$$

と書けることがわかる．　　定理1.2の証明終わり□

参考文献

[1] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms.* Undergraduate Texts in Mathematics. Springer-Verlag, 1992.

[2] S. G. Simpson. *Subsystems of Second Order Arithmetic.* Perspectives in Mathematical Logic. Springer-Verlag, 1999.

[3] 坂本伸幸, 田中一之. 2階算術における実数と複素数. 圏論と証明論の新しい融合を目指して, 数理解析研究所講究録, 本巻. 京都大学数理解析研究所, 2001.

[4] 中野茂男. 復刊 代数幾何学入門. 共立出版, 1999.